Introducing the Next-Generation Common Access Card

By Sonya R. Smith

The Department of Defense (DoD) is modifying the current Common Access Card (CAC) to meet the mandates of Homeland Security Presidential Directive 12 (HSPD-12). HSPD-12 establishes a federal standard for identification credentials issued to all federal employees and eligible contractors.

The "next-generation CAC" is being phased in throughout the DoD as current CACs expire. During this transition period, both the current Common Access Card, and the next-generation CAC will be in circulation. Both are valid forms of identification and there is no benefit to replacing your current card with a next-generation CAC before its expiration date.

The next-generation CAC maintains all the capabilities and functionality of the current card: data stored on an integrated circuit chip (ICC) enables rapid electronic authentication and enhanced security. PKI certificates generated and stored on the card enable the card owner to digitally sign documents and e-mails, encrypt e-mails, and establish secure online network connections.

Added Functionality

Instead of having to stop and "swipe" your card to read the information from the magnetic stripe or bar code, the next-generation CAC adds a contactless technology capability, which provides the ability to utilize radio frequencies to transfer data between the card and the card reader for physical access. This increases the speed for identity authentication and improves the ability to manage heavy traffic flow into facilities.

In addition to the PKI certificates, the next-generation CAC adds biometrics in the form of a digital photo and two index fingerprints, stored as minutiae templates on the ICC. The minutiae templates are a mathematical representation of the data points unique to each set of biometrics. They are used instead of storing actual fingerprint images on the next-generation CAC to protect against compromise.

Biometrics provide the ability to positively bind the individual to his or her credential. The integration of biometrics and PKI with the CAC provides an added multifactor authentication capability for logical and physical access systems.

Multifactor authentication, which relies on more than one means to authenticate identity, is a more robust authentication scheme because it requires possession of a particular item — the CAC; knowledge of a particular item — your Personal Identification Number (PIN); and physical verification — biometrics.

Changes in Appearance

The look of the next-generation CAC will change slightly to meet federal standards and to better meet security needs. Figure 1 shows a depiction of the current CAC on the left and the next-generation CAC on the right. The following are the key differences you will see with the next-generation CAC:

Color Coding:

- *A red stripe will be used to represent first responders. Red is used to identify foreign nationals on current CACs.*
- *A blue stripe will be used to represent foreign nationals.*
- *A green stripe will continue to represent contractors.*
- *The stripe will be horizontal under the photo and fade from light to dark. Currently the stripe is vertical on the right side.*

Data Storage

Contrary to popular belief, the CAC does not store any personal or medical records. The next-generation CAC requires increased storage capacity simply to store the biometrics and the federally required Personal Identity Verification (PIV) certificate. The goal, in our net-centric world, is to use the card, with its PKI and biometrics as identity authentication factors, to access authoritative data sources through Web portal applications. Below is a summary of the key data included in the technology of the card.

The integrated circuit chip stores 64 kilobytes of data, including:

- PKI certificates
- Two digital fingerprints (minutiae templates)
- Digital photo
- Personal Identity Verification (PIV) certificate
- Organizational affiliation
- Agency
- Department
- Expiration date

Bar codes may store key personal information, including:

- Name
- Social Security Number
- Date of birth
- Personnel category
- Pay category
- Benefits information
- Organization affiliation
- Pay grade

The magnetic stripe is reserved for Service/Agency use.

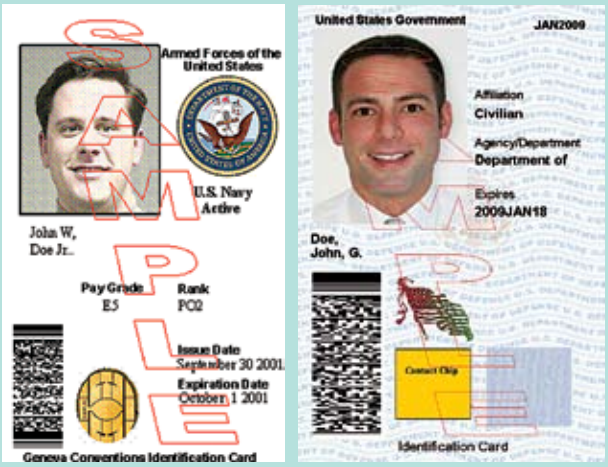

Figure 1 depiction of the current CAC and next-generation CAC.

Getting the Card – Changes to the Process

One of the key mandates of HSPD-12 is that the identity credential must be issued based on sound criteria for verifying an individual's identity. Accordingly, a next-generation CAC can only be issued when a National Agency Check with Inquiries, or equivalent, is submitted and the results of the FBI National Criminal History Check (fingerprint check) have been completed and approved.

When a record has been established in the Defense Enrollment Eligibility Reporting System (DEERS) and the FBI fingerprint check has been completed and approved, individuals must bring two forms of approved identity source documents with them for CAC issuance. *Go to http://www.cac.mil for a list of approved identity documents.*

At least one document must be a valid state or federal government–issued picture identification, such as a passport, driver's license or current/expired CAC. Additionally, just as with the current CAC, you will need a six- to eight-digit PIN and an official work e-mail address in order to receive all your PKI certificates.

Impact to Users

The next-generation CAC requires upgrades to our current middleware infrastructure — the software application that interfaces between host applications, such as e-mail, cryptographic logon, Web browsers, and PK-enabled applications, and the CAC. While DoD upgrades the infrastructure to produce the next-generation CAC, new cardstock is being introduced for the current CAC to replace depleted cardstock inventories.

This new cardstock also requires upgraded middleware for proper functionality. NMCI is upgrading the CAC middleware from ActivClient 5.4 to ActivClient 6.0 during the first quarter of 2007. This upgrade makes NMCI compliant with industry standards and provides support for the next-generation CAC.

If users are issued a CAC with the new cardstock or a next-generation CAC before their NMCI workstation has been upgraded to ActivClient 6.0, they may not be able to use their newly issued CAC on their workstation. Should this occur, the affected users should call the NMCI Help Desk (866-THE-NMCI), indicate they were recently issued either a CAC with the new cardstock or a next-generation CAC, and the NMCI Help Desk will push the ActivClient 6.0 upgrade to the user's workstation. Users not on NMCI who are using ActivIdentity 2.2 should not be affected.

Because the CACs created with the new cardstock look identical to the current version of the CAC, users will only be able to identify the new cardstock by the manufacturer and card type indicated on the back of the CAC. If the CAC reads "Oberthur Card Systems ID-One Cosmo v5.2 72K" above the magnetic bar on the back of the CAC, then the user has the new cardstock.

Users will be able to more easily identify the next-generation CAC because this card will look different from the current version of the CAC, as illustrated in Figure 1.

Different but the Same

The CAC has been well integrated into the DoD with military members, civilians and contractors using it for logical and physical access and digitally signing and encrypting e-mail. It is also used as the standard ID card and Geneva Convention Card.

The next-generation CAC builds upon a proven record of success and meets the federal standards of HSPD-12. Issuance of next-generation CACs began in October 2006 with an Interim Operational Capability solution and will be phased in throughout the DoD as current CACs expire. While there are differences in appearance and functionality, both the current CAC and the next-generation CAC are valid forms of DoD identification.

Ms. Sonya Smith supports the DON CIO information assurance team.

CHIPS

Go to the following Web sites for further guidance:

- HSPD-12, Homeland Security Presidential Directive, August 27, 2004, Subj: Policy for a Common Identification Standard for Federal Employees and Contractors: http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.
- FIPS201-1 – Federal Information Processing Standard 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006: http://csrc.nist.gov/.
- DoD Common Access Card Web site: http://www.cac.mil.